Attorney Docket No.: 20976-2.00US

PATENT APPLICATION

IDENTITY VERIFICATION USING BIOMETRICS

Inventor:

Shawn J. Bradley, a citizen of United States, residing at,
3314 Stephens Avenue
Missoula, MT 59801

Richard F. Peralta, a citizen of United States, residing at,
4618 Watt Lane
Stevensville, MT 59870

Business: Small entity

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel: 650-326-2400

IDENTITY VERIFICATION USING BIOMETRICS

BACKGROUND OF THE INVENTION

The present invention relates to identity verification systems, and more particularly to identity verification systems based on biometrics.

The use of a token to effectuate financial transactions has become more pervasive in today's financial market. A token, such as a debit or credit card, typically identifies both the account holder as well as the account that is the subject of the financial transaction.

The rise in the number and types of accounts accessible by, for example, a debit or credit card has seen a parallel increase in the level of criminal activities related to unauthorized use of such credit or debit cards. Credit card fraud, which occurs in many different forms, often largely arises as a result of either stolen or counterfeit cards.

Typically, debit cards are used in conjunction with a personal identification number (PIN). A PIN is designed to prevent unauthorized use of lost or stolen cards. However, a number of techniques have been used by unauthorized users to obtain PINs from unwary cardholders. Such techniques include, for example, using Trojan horse automated teller machines (ATMs) that dispense cash but record the PINs, using fraudulent debit devices that also record the PINs, or watching the account holder enter a selected PIN into an ATM with the aid of binoculars. A PIN obtained via any of the above techniques is subsequently used in a counterfeit card to fraudulently withdraw funds from the targeted account.

Fraud committed by account holders is also on the rise. An account holder may withdraw cash from the account--with the card which is in his possession--and deny responsibility for the withdrawal by claiming that he had lost the card--on which he claims he had written the PIN associated with the card--and thus asserting that someone else withdrew cash from the account.

In an effort to improve the security and reliability of token-based transactions, new techniques have been developed. In accordance with one technique, a binary number extracted from an authenticated biometric--taken from the account holder to whom the token is issued--is stored on the token. To gain access to the account and thus to carry out a transaction, the token holder is required to supply the requested biometric at the transaction

site. Data extracted from the biometric supplied at the transaction site by the token holder is then compared to the data stored on the token to determine if the two match. If a match exists between the two data, the token holder's identity is verified and access to the account is authorized.

Various biometrics have been considered for use with smartcards, such as fingerprints, hand prints, voice prints, retinal images, handwriting samples and the like. An example of a biometric-based smartcard is found in U.S. Pat. No. 5,280,527 issued to Gullman et al. which disclose a credit card sized token (referred to as a biometric security apparatus) containing a microchip in which a sample of the authorized user's voice is stored. In order to gain access to an account, the user must insert the token into a designated slot of an ATM and then speak to the ATM. If a match is found between the user's voice and the sample recording of the voice stored on the microchip, access to the account is granted. Alternatively, the ATM may prompt the user for an additional code, such as a PIN which is also stored on the token, in order to authorize account access.

Although Gullman et al' system reduces the risk of unauthorized access when compared against conventional PIN-based systems, to the extent that the credit card and the microchip disposed therein may be tampered with, Gullman's system does not provide the level of reliability and security that is often required in today's highly diverse and ever expanding financial transactions.

SUMMARY OF THE INVENTION

In accordance with the present invention, an authorization system grants access to an account only if (i) a biometric image stored on a microchip disposed on a token matches a biometric image supplied by the token holder at the time and site of the transaction and (ii) data associated with and extracted from the biometric image supplied by the account holder--prior to the issuance of the token--matches a corresponding data associated with and extracted from either the biometric image stored on the microchip or that supplied by the user at the transaction site.

In some embodiments of the present invention, the token is a card and the biometric is a finger print. The microchip stores the finger print image in, for example, bitmap, Tiff or JPEG format. The data extracted from the finger print's image is, for example, 8 bits wide and is stored in a database that may be physically located away from the transaction site.

To request access to an account from a transaction site, a cardholder first supplies his card to a computer system located at the transaction site. The cardholder is then instructed to place his finger on a scanner, thereby to capture the cardholder's finger print image. An image of the same finger print captured prior to the issuance of the card is stored inside a microchip on the card. If a match exists between the finger pint image stored in the microchip and that supplied by the cardholder at the transaction site, the system proceeds to the second phase of the verification.

During the second verification phase, previously extracted security data stored in a database is compared with a corresponding data extracted from either the finger print image stored in the microchip or the finger print supplied by the user at the transaction site. If there is a match between the two data compared during the second verification phase, then access to the account is granted if the account meets certain qualifying requirements.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a front view of a token, in accordance with one embodiment of the present invention.

Fig. 2 is a perspective view of an authorization terminal, in accordance with one embodiment of the present invention.

Fig. 3 is a flowchart illustrating the process during a first phase of authorization of access to an account, in accordance with one embodiment of the present invention.

Fig. 4 is a flowchart illustrating the process during a second phase of authorization of access to an account, in accordance with one embodiment of the present invention.

DESCRIPTION OF THE SPECIFIC EMBODIMENTS

Fig. 1 is a front view of token 10, in accordance with one embodiment of the present invention. Token 10 includes a body 20 which may be formed from, for example, plastic, metal, or the like. Body 20 further includes integrated circuit (hereinafter alternatively referred to as microchip) 30 in which an image of, for example, the finger print of the person to whom the card is issued (hereinafter referred to as the account holder) is

stored. The finger print image is stored in microchip 30 in one of many commercially available formats such as, Tiff, JPEG, bitmap, etc. Token 10 optionally includes a data carrying medium 40 in the form of raised symbols that contain additional data related to the account for which token 10 is issued. Such data may include, for example, credit or debit account number or the like.

Token 10 optionally also includes mediums 50 and 55 as well as magnetic stripes 60 on which account related data may also be stored. Medium 50 may include such information as the name or the logo of the entity issuing or affiliated with token 10. Medium 55 may include, for example, a hologram on which parts of the raised symbols of data carrying medium 40 are positioned. Magnetic stripes 60 include such information as the name or the address of the account holder, etc.

Although, the biometric image stored in microchip 30 is a fingerprint image, it is understood that other biometrics such as hand prints, retinal images, handwriting samples and the like may also be stored in microchip 30, in accordance with the present invention.

Token 10 is provided to the account holder by an issuing entity, such as a bank, a credit card company, an agency. For example, token 10 may be a credit card or debit card issued by a bank or it may be a driver's license issued by the department of motor vehicles, etc.

To receive token 10 in connection with an account, the person requesting the token (i.e., the account holder) submits a biometric, such as a fingerprint, to the token issuing entity, such as a bank. Submission of, for example, a finger print may be carried out in many different ways. For example, the issuing entity may mail a form to the account holder. The account holder fills out the questions asked on the form and supplies his finger print in a designated space on the form and as directed thereby. Thereafter, the account holder sends the completed form to the issuing authority. The account holder's finger print image is electronically scanned and captured by an image processing system and subsequently digitized and stored in a memory. Alternatively, the account holder may visit a registration station--administered by the issuing entity--to provide his finger print. The finger print is scanned and captured by an image processing system and subsequently digitized and stored in a memory.

The stored finger print image--obtained via either of the above methods--is thereafter centered, deskewed and sized. According to the present invention, additional security is provided by a second verification phase, during which secondary data matching is required. In one embodiment, this is accomplished by extracting the data from the finger print

image. Specifically, in accordance with a preselected algorithm, a binary number is generated from the stored finger print image and is permanently stored in a database controlled by the issuing authority.

A copy of the stored finger print image is subsequently transferred to and stored in microchip 30 for future account access authorizations. The finger print image stored in microchip 30 may be in one of many commercially available formats, such as, Tiff, JPEG or bitmap. The image stored in microchip 30 is subsequently compared with the finger print image of the token holder taken at the transaction site whenever request to access the account is made by the token holder, as described further below.

Fig. 2 is a perspective view of an authorization terminal 70, in accordance with one embodiment of the present invention. Terminal 70 is positioned in a point of sale or a site where financial transactions and thus access to accounts occur. Terminal 70 includes, among other components, a slot 80 adapted to receive token 10 and to read data stored in microchip 30 disposed thereon. Slot 80 may also be adapted to read account related information stored, for example, on magnetic stripes 60.

Terminal 70 further includes a biometric sampler, such as a biometric scanner 90, that communicates with other components of terminal 70 through a port 100. If the biometric selected for account access is a finger print, scanner 90 is a fingerprint scanner, as known in the art. Terminal 70 receives power through a power port 110. Terminal 70 optionally includes a display, such as a light emitting diode (LED) display 120 and a keypad 130. Terminal 70 also includes a processor therein (not shown).

Such a processor may be configured to perform a number of functions. Such functions are typically performed by software code modules stored in a memory and executed by the processor. Alternatively, such functions may be carried out by specialized logic hardware modules (not shown). Still in other embodiments, such functions may be carried out by software modules executed by the processor in conjunction with other logic hardware modules.

Fig. 3 is a flowchart illustrating the process of accessing an account during the first phase of identity verification, in accordance with one embodiment of the present invention. At initial step 300, token 10 is inserted into slot 80 of terminal 70, thereby causing the processor to read the finger print image data stored in microchip 30 of token 10. Thereafter, at step 330, in accordance with a preselected algorithm, the processor generates a binary number (hereinafter referred to as the first binary number) from the finger print image data stored in microchip 30.

At step 350, the token holder is instructed to place the finger, from which a print was taken earlier, on scanner 90. At step 360, the finger print is scanned by scanner 90 which is coupled to an image capture system (not shown), such as a camera system, thereby forming an image of the finger print. The scanned finger print image is subsequently formatted, i.e., centered, deskewed and sized by the processor. Thereafter, at step 370, in accordance with the preselected algorithm, the processor generates a binary number (hereinafter referred to as the second binary number) from the finger print image that was scanned by scanner 90 and was subsequently centered, deskewed and sized by the processor and the image capture system.

At step 390 the processor compares the first and second binary numbers to determine whether they match each other within a predefined tolerance limit. If there is a match, then at step 395 the processor extracts a predefined portion of either the first or the second binary numbers and stores the extracted portion (hereinafter referred to as the third binary number) in a memory. It is understood that the third binary number may be encrypted in a manner known in the art. Furthermore, it is understood that the third binary number may be formed from either contiguous or non-contiguous bits of the first or the second binary numbers. If a match is found between the first and second binary numbers, the identity verification or account access authorization proceeds to the second phase, as shown by step 400.

If no match is found between the first and second binary numbers, then at step 410 a counter (not shown) is incremented and the process returns to step 360 at which point the card holder's finger print is scanned again to from a new image therefrom, as described above. The process is so repeated, for example, 20 times or until a match occurs between the first and second binary numbers. Each scanned image of the card holder's fingerprint is saved in a temporary memory. If, for example, after 20 repeats of step 360 (i.e., i>20), no match is found between the first and second binary numbers, then at step 420, access to the account is denied and a message indicating the denial appears on display 120, at which point the process of accessing the account is terminated. If the process is so terminated, then at step 430 the scanned images of the cardholder's fingerprint is delivered from the temporary memory to a relatively more permanent memory for possible transfer to law enforcement agencies.

As shown in Figs. 3 and 4, if a match exists between the first and second binary numbers, account access authorization proceeds to step 440 at which point additional account information stored in token 10 may be read therefrom. Such additional account information which may include, for example, the account number, the name and the address

of the account holder, or the like, may be also stored in, for example, microchip 30, medium 40 or the magnetic stripes 60, as described above.

If such additional information is stored in a magnetic stripe, the token holder may be instructed to remove token 10 from slot 80 and swipe the token through slot 80. Alternatively, token 10 may be swiped through another opening formed in terminal 70, thereby to enable a magnetic read device (not shown) to read any information stored on the magnetic stripe, as known in the prior art. The cardholder may be instructed to place token 10 in or remove token 10 from slot 80 by, for example, a message shown on display 120, or by an audible signal generated by a speaker (not shown) attached to terminal 70.

At step 450, the third binary number is appended to any account information that is read at step 440. The third binary number and any account information appended thereto is subsequently transmitted to another computer system (not shown) under the control of the issuing entity and which may be stationed at a different physical location than terminal 70.

At step 460, the computer system receives and separates the third binary number from any account information appended thereto. The computer system also retrieves the binary number that is stored in the database (hereinafter referred to as the fourth binary number) and which is controlled by the issuing entity, as described above. Thereafter, the computer system compares the third and fourth binary numbers to determine whether they match. If the third and fourth binary numbers match within a predefined tolerance limit, the process moves to step 470, described below.

If, on the other hand, no match is found between the third and fourth binary numbers within the predefined tolerance limit, access to the account is denied and the transaction attempt is terminated, a shown in step 480. Furthermore, at step 480, a message corresponding to this denial is displayed on display 120 or broadcast via the speakers attached to terminal 70.

If the process is so terminated, then at step 490, the scanned images of the token holder's finger print images are stored in a permanent memory for possible transfer to law enforcement agencies. Furthermore, terminal 70 is then reset for the next transaction.

If there is a match between the third and fourth binary numbers, identity verification is successful. Accordingly, as indicated in step 470, the account is analyzed to determine whether it meets one or more qualifying requirements (e.g., account is not overdrawn, credit limit not exceeded, token holder is authorized entry, etc.). If the account meets the qualifying requirements, as shown in step 500, the desired account transaction

occurs and a verified code or other information indicating acceptance of the transaction is generated and transmitted to display 120. Subsequently, at step 530 the temporary memory which stores the fingerprint images taken at the transaction site is erased. Terminal 70 is similarly reset for the next transaction.

If the account qualifying requirements are not met, then at step 510, a transaction denied signal is generated and transmitted to display 120 and the account access process is terminated. If the process is terminated, then at step 520 the temporary memory which stores the fingerprint images taken at the transaction site is erased. Terminal 70 is similarly reset for the next transaction.

Although the invention has been described in terms of the illustrative embodiment, it is understood by those skilled in the art that various changes and modifications may be made to the illustrative embodiment without departing from the spirit or scope of the invention. For example, terminal 70 may incorporate or be used in conjunction with a point-of-sale token reader known in the art.

It is understood that token 10 may include, in addition to credit/debit cards, a passport, driver license, or door/zone access card. The scope of the present invention is not limited in any way to the illustrative embodiment shown and described.

For purposes of the present invention, the term "account" is to be broadly construed to include a right or rights accessible based on positive user identification, such as, but not limited to, financial accounts, driving privileges, foreign travel privileges, access to restricted areas and the like.

The drawing figures are intended to illustrate the general manner of construction and are not to scale. In the description and in the claims, the terms left, right, front and back and the like are used for descriptive purposes. However, it is understood that the embodiment of the invention described herein is capable of operation in other orientations than are shown and the terms so used are only for the purpose of describing relative positions and are interchangeable under appropriate circumstances.